EXHIBIT 3

IN THE UNITED STATES DISTRICT COURT FOR
THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, et al.	)	
Plaintiff,	)	**CIVIL ACTION FILE NO.:** **1:17-cv-2989-AT**
vs.	)	
BRIAN P. KEMP, et al.	)	
Defendant.	)	

DECLARATION OF RICHARD A. DeMILLO

RICHARD A. DeMILLO hereby declares as follows:

1. This statement supplements my declaration of August 20, 2018 addressing the Defendants' incorrect and misleading assertion that the phrase "undetectable manipulation" has been manufactured to suit the present lawsuit by the Plaintiffs "for the convenient reason that it dodges any test for corroboration."
2. In that declaration I noted that undetectable manipulation is the aim of Advanced Persistent Threats ("APT") and pointed out that the publicly

announced consensus view of U.S. intelligence agencies and legislative committees that have access to classified threat information is that APTs are responsible for past and continuing efforts to scan, penetrate, manipulate and disrupt the American election system.

3. I also cited the many textbooks that analyze the various mechanisms that such threats might use to avoid detection. Although techniques for discovering the presence or activity of malware that seeks to cover its tracks through stealth are the basic building blocks of cybersecurity education, students are taught that malware may be undetectable either because proper countermeasures have not been deployed or because the countermeasures are not effective.

4. On September 6, 2018, the National Academy of Sciences, Engineering, and Medicine and the associated National Research Council (NAS) issued a report entitled "Securing the Vote: Protecting American Democracy" [National Academies Publication 25120, Attached as Exhibit 1]. Had the NAS report been publicly available, I would have cited it in my August 20 declaration.

5. I now wish to supplement that declaration to include references to the NAS report.

Executed on this date, September 9, 2018.

Richard A. DeMillo

EXHIBIT 1

Securing the Vote

Protecting American Democracy

Committee on the Future of Voting:
Accessible, Reliable, Verifiable Technology

Committee on Science, Technology, and Law

Policy and Global Affairs

Computer Science and Telecommunications Board

Division on Engineering and Physical Sciences

A Consensus Study Report of

The National Academies of
SCIENCES · ENGINEERING · MEDICINE

THE NATIONAL ACADEMIES PRESS
Washington, DC
www.nap.edu

BOX 3-2
The Role of Paper in Elections

Until the widespread adoption of mechanical lever machines in the mid-20th century, hand-marked paper had been the most common medium upon which a voter cast a ballot. The cast paper ballot provided a physical record that could be examined in instances where a recount or other reconciliatory action was required. With the advent of mechanical lever machines, no record of a voter's choices was permanently stored, either on paper or mechanically—the only effect of casting a vote was to increment mechanical counters that accumulated the choices made by voters on a particular machine. Mechanical lever machines were popular where they were used. However, these machines were prone to breakdowns that could go undetected until balloting had ended.

Before the passage of the Help America Vote Act (HAVA), it was common for jurisdictions with lever machines to adopt electronic systems when they considered upgrading their voting systems. HAVA provided an impetus for jurisdictions that had previously used lever machines to adopt Direct Recording Electronic systems (DREs), either to provide accessible options for those with disabilities, or to replace paper-based systems altogether. The rapid growth in the prominence of DREs brought greater voice to concerns about their use, particularly their vulnerability to software malfunctions and external security risks. And as with the lever machines that preceded them, without a paper record, it is not possible to conduct a convincing audit of the results of an election.

Many electronic voting systems utilize paper as part of their operation. As discussed in Box 3-1, voters may mark paper ballots that are subsequently recorded electronically by scanning devices. Alternatively, ballot-marking devices may be used to mark paper ballots according to voters' instructions. In the case of DREs, there is no physical (i.e., paper) ballot. Instead, the ballot exists only in electronic form.

Problems arise when a voter does not actually verify his or her ballot, especially when the ballot is being tabulated by a computer that has a software flaw or is infected with malware (see Chapter 5). A ballot that is "voter marked" is by definition voter verified. Voters can verify that the selections on hand-marked ballots or on paper ballots produced by BMDs reflect their intended choices before their votes are tabulated. With DREs, voters may similarly verify their selections using a voter-verifiable paper audit trail (VVPAT) (see Box 3-1)—provided that the DRE is equipped with this feature. The information on a VVPAT may accurately present a voter's selections, but VVPATs exist independently of the record maintained in the DRE's computer memory. In most cases it is the electronic record, and not the VVPAT, that is used for vote tabulation.[a]

Paper Ballots Defined

Because records of ballots may take many forms, it is important to clearly define what is meant by "paper ballot." For the purposes of this report, references to paper ballots refer to original records that are produced by hand or a ballot-marking device, which are human-readable in a manner that is easily accessible for inspection and review by the voter without any computer intermediary (i.e., Voters may inspect a VVPAT to see whether it reflects their intended selections before their votes are recorded in computer memory. If voters do not verify that the information on their VVPAT is accurate, inaccuracies may be recorded. Those with vision or other impairments or limitations may not, however, be able to perform this inspection. Furthermore, it may be difficult to track patterns of VVPAT errors that would indicate fraud. Finally, a combined approach that uses DREs and printers introduces complexity and adds new points of potential failure at the polling place.

Jurisdictions typically transmit ballots to those wishing to cast ballots via mail. Ballots may sometimes be retrieved from an elections website for printing and completion by remote voters. Some jurisdictions may also provide remote voters with software to prepare their ballots. While this software avoids problems associated with manual use of paper ballots such as undervotes and overvotes and spoiled ballots (as voters get immediate feedback before completing their ballots), it introduces additional security risks. Completed ballots are returned via mail, at designated collection points, or, in certain instances, by fax or via the Internet.

Well designed, voter-marked paper ballots are the standard for usability for voters without disabilities. Research on VVPATs has shown that they are not usable/reliable for verifying that the ballot of record accurately reflects the voter's intent, but there is limited research on the usability of BMDs for this purpose. BMDs moreover, may produce either a full ballot, a summary ballot, or a "selections-only" ballot. Unless a voter takes notes while voting, BMDs that print only selections with abbreviated names/descriptions of the contests are virtually unusable for verifying voter intent.[75]

Human beings must, however, interact not only with ballots, but also with all components of election systems. A usability failure of any particular component of an election system can be as detrimental as a failure of usability in the ballot. A voting system must be usable in a way that allows a voter to verify that the ballot of record correctly reflects his or her intent. Vote tabulation systems must be usable in a way that facilitates the correct tallying and tabulation of votes. Auditing technology must be useable in a way that enables efficient recounting.

Findings

Not all voting systems have the capacity for the independent auditing of the results of vote casting. Electronic voting systems that do not produce

[75] By hand marking a paper ballot, a voter is, in essence, attending to the marks made on his or her ballot. A BMD-produced ballot need not be reviewed at all by the voter. Furthermore, it may be difficult to review a long or complex BMD-produced ballot. This has prompted calls for hand-marked (as opposed to BMD-produced) paper ballots whenever possible.

a human-readable paper ballot of record raise security and verifiability concerns.

The software for casting and tabulating votes is not uniformly independent in voting systems.

Voting technology raises a particular set of issues for the disabled community.

Additional research on ballots produced by BMDs will be necessary to understand the effectiveness of such ballots.

RECOMMENDATIONS

4.10 States and local jurisdictions should have policies in place for routine replacement of election systems.

4.11 Elections should be conducted with human-readable paper ballots. These may be marked by hand or by machine (using a ballot-marking device); they may be counted by hand or by machine (using an optical scanner).[76] Recounts and audits should be conducted by human inspection of the human-readable portion of the paper ballots. Voting machines that do not provide the capacity for independent auditing (e.g., machines that do not produce a voter-verifiable paper audit trail) should be removed from service as soon as possible.

4.12 Every effort should be made to use human-readable paper ballots in the 2018 federal election. All local, state, and federal elections should be conducted using human-readable paper ballots by the 2020 presidential election.

4.13 Computers and software used to prepare ballots (i.e., ballot-marking devices) should be separate from computers and software used to count and tabulate ballots (scanners). Voters should have an opportunity to review and confirm their selections before depositing the ballot for tabulation.

VOTING SYSTEM CERTIFICATION

Overview and Analysis

Under HAVA, the EAC became responsible for developing and administering a voluntary system for federal certification of voting systems.[77] These

[76] A modern form of optical scanner, a *digital scanner,* captures, interprets, and stores a high-resolution image of the voter's ballot at a resolution of 300 dots per inch (DPI) or higher.

[77] U.S. Election Assistance Commission, "Testing & Certification Program Manual, Version 2.0," available at: https://www.eac.gov/assets/1/6/Cert_Manual_7_8_15_FINAL.pdf.

guidelines, known as the Voluntary Voting System Guidelines (VVSG), specify certain functional, accessibility, and security requirements for voting systems.

The EAC has two responsibilities pertinent to certification. First, with the technical assistance of the National Institute of Standards and Technology (NIST), the EAC oversees the development of the VVSG, which establishes the standards against which new voting systems are tested. Second, the EAC certifies independent voting system testing laboratories (VSTLs), which conduct the testing of new voting systems developed by commercial vendors.

States are ultimately responsible for determining the process by which voting systems will be certified in their states. Thirty-eight states and the District of Columbia rely on the federal testing and certification program, at least to some extent.[78] This can range from requiring that systems be tested to federal standards to requiring that systems be tested in federally approved laboratories. The remaining states do not require federal testing or certification per se, but in most cases rely on the federal certification program to guide their own state certification regimes. HAVA envisioned that the states might also perform testing of the accuracy, usability, and durability of the systems that they proposed to put into service.

The federal certification process begins only once a manufacturer has registered with the EAC Voting System Testing and Certification Program and has submitted a system for certification.[79] The process of certification can take up to 2 years. [80] Even then, a state certification process frequently follows after federal certification has been received. Following certification, other procedures, such as acceptance testing, logic and accuracy testing, and special purpose tests may follow. All told, the period between the develop-

[78] See National Conference of State Legislatures, “Voting System Standards, Testing, and Certification,” available at: http://www.ncsl.org/research/elections-and-campaigns/voting-system-standards-testing-and-certification.aspx.

[79] See “Testing & Certification Program Manual, Version 2.0.” Systems are usually “submitted when (1) they are new to the marketplace, (2) they have never before received an EAC certification, (3) they are modified, or (4) the Manufacturer wishes to test a previously certified system to a different (newer) standard.” See p. 19.

[80] Perez, Eddie, Hart InterCivic and Coutts, McDermot, Unisys Voting Solutions, presentations to the committee, December 8, 2017, Denver, CO. See also University of Pennsylvania, Wharton Public Policy Initiative, “The Business of Voting: Market Structure and Innovation in the Election Technology Industry,” 2016, p. 38, available at: https://publicpolicy.wharton.upenn.edu/live/files/270-the-business-of-voting.

ment of a new voting systems and its actual use in an election can last years and cost vendors millions of dollars.[81]

Current security standards certify equipment but not associated procedures and procedural requirements (e.g., auditing). This fact contributes to deficiencies in current standards.

Newly revised voluntary voting system guidelines, called VVSG 2.0, await final approval from the EAC. The new guidelines provide a more modular set of specifications and requirements against which voting systems can be tested to determine whether the systems provide basic functional, accessibility, and security capabilities required of these systems. This change is intended to foster the deployment of accurate and secure voting systems while also enabling system innovation that would allow the deployment of system upgrades in a timely fashion, facilitate interoperability of election systems, permit the transparent assessment of the performance of election systems, and provide a set of testable requirements that are easy to use and understand.[82] The approach of VVSG 2.0 focuses more on functional requirements than on the prescriptive specifics of the past. The draft guidelines require software independence for all voting systems in order to allow the correct outcome of an election to be determined even if the software does not perform as intended.[83,84]

Findings

Vendors and election administrators have expressed frustration with the certification process as presently implemented.

Costs and delays in the certification process may limit vendor innovation and increase system costs.

The requirements of the certification system can create barriers to

[81] The software used in voting systems is also subject to certification. This has important implications for system security. If the most recent version of particular software has not been certified, states may be forced to use an earlier software version with documented vulnerabilities.

[82] U.S. Election Assistance Commission, "VVSG Version 2.0: Scope and Structure," available at: https://www.eac.gov/assets/1/6/VVSGv_2_0_Scope-Structure(DRAFTv_8).pdf.

[83] "A voting system is software independent if an (undetected) change or error in its software cannot cause an undetectable change or error in an election outcome." See Rivest, Ronald L., "On the Notion of 'Software Independence' in Voting Systems," *Philosophical Transactions of the Royal Society A*, October 28, 2008, DOI: 10.1098/rsta.2008.0149. Dr. Rivest is a member of the committee that authored the current report.

An auditable voting system is software independent.

[84] The auditing of election results can reduce the need for certification and simultaneously provide better evidence that outcomes are correct. See, e.g., Stark, Philip B. and David A. Wagner, "Evidence-Based Elections," *IEEE Security and Privacy*, 2012, Vol. 10, DOI 10.1109/MSP.2012.62.